Peng Xue, Chuan-Feng Li* , and Guang-Can Guo†
Laboratory of Quantum Communication and Quantum Computation and Department of Physics, University of Science and Technology of China, Hefei 230026, P. R. China

We propose an efficient quantum key distribution scheme based on entanglement. The sender chooses pairs of photons in one of the two equivalent nonmaximally entangled states randomly, and sends a sequence of photons from each pair to the receiver. They choose from the various bases independently but with *substantially* different probabilities, thus reducing the fraction of discarded data, and a significant gain in efficiency is achieved. We then show that such a refined data analysis guarantees the security of our scheme against a biased eavesdropping strategy.

PACS numbers: 03.65.Ud, 03.67.Dd

I. INTRODUCTION

Cryptography is the art of providing secure communication over insecure communication channels. To achieve this goal, an algorithm is used to combine a message with some additional information—known as the "key"—to produce a cryptogram. For this reason, secure key distribution is a crucial problem in cryptography.

Since the publication of BB84 scheme proposed by Bennett and Brassard, there has been much interest in using quantum mechanics in cryptography [1–8]. The security of these quantum key distribution (QKD) schemes is based on the fundamental postulate of quantum physics that "every measurement perturbs a system". Indeed, passive monitoring of transmitted signals is strictly forbidden in quantum mechanics. The "quantum no-cloning theorem" [9,10] indicates that it is impossible to make an exact copy of an unknown quantum state.

Two well-known concepts for quantum key distribution are the BB84 scheme [1] and the Ekert scheme [2]. The BB84 scheme [1] uses single photons transmitted between two parties (commonly called Alice and Bob). The sender Alice uses non-orthogonal quantum states to transfer the key to the receiver Bob. Such states cannot be cloned, hence any attempt by an eavesdropper, known as Eve, to get information on the key disturbs the transmitted signals and induces noise which will be detected during the second stage of the transmission. Alice and Bob randomly pick a subset of photons from those that are measured in correct bases and publicly compare their measurements. For these results, they estimate the average error rate $\overline{e}$. If $\overline{e}$ turns out to be unreasonably large, then eavesdropping has occurred, all the data are discarded and they may re-start the whole procedure.

The Ekert scheme [2] is based on entangled pairs and uses the generalized Bell's inequality (Clauser-Horne-Shimony-Holt inequality) [11,12] to establish security. Both Alice and Bob receive one particle out of an maximally entangled pair. They perform measurements along at least three different directions on each side, where measurements along parallel axes are used for key generation and oblique angles used for testing the inequality

Neither scheme described above which is based on non-orthogonal quantum cryptography has an efficiency more than 50%. Recently, Lo *et al.* devise a modification [13] that essentially doubles the efficiency of the BB84 scheme, where, Alice and Bob choose between the two bases independently but with *substantially* different probabilities ϵ and $1-\epsilon$. They also prove the security of their scheme.

In this paper, we present a new efficient QKD scheme with nonmaximally entangled states. Suppose Alice creates pairs of photons in the nonmaximally entangled state $|AB\rangle$ which can be transformed to its equivalent state $|AB\rangle'$ with the same Schmidt coefficients by local unitary transformations. She chooses pairs of photons in one of the two states randomly, and sends a sequence of photons out of each pair to Bob. The two users choose their bases independently with different probabilities and perform measurements. Similar to the scheme proposed by Lo *et al.*, as two parties are much more likely to be using the same basis, thus reducing the fraction of discarded data, a significant gain in efficiency is achieved. To ensure our scheme is secure, we separate the accepted data into various subsets according to the basis employed and estimate an error rate for each subset *separately*. We show that the refined error analysis is sufficient in ensuring the security of our scheme against "a biased eavesdropping attack" [13].

*Email address: cfli@ustc.edu.cn
†Email address: gcguo@ustc.edu.cn

In next section, we give the detailed description of our efficient QKD scheme with nonmaximally entangled states. By considering a simple biased eavesdropping strategy by Eve, we note that our refined analysis is an essential feature of our scheme in Sec. III. In Sec. IV, the constraint on the probability ϵ is derived. Finally, we conclude the scheme in Sec. V.

II. EFFICIENT QKD SCHEME WITH NONMAXIMALLY ENTANGLED STATES

In our scheme, there are two parties: the sender, Alice and the receiver, Bob. Alice prepares pairs of photons in the nonmaximally entangled state

$$|AB\rangle = \alpha |H\rangle_A |H\rangle_B + \beta |V\rangle_A |V\rangle_B \tag{1}$$

where $|\alpha|^2 + |\beta|^2 = 1$, and H and V denote the horizontal and vertical linear polarization, respectively. Then she performs two "σ_x" operations on the two particles respectively to transform the state $|AB\rangle$ to its equivalent state

$$|AB\rangle' = \beta |H\rangle_A |H\rangle_B + \alpha |V\rangle_A |V\rangle_B \tag{2}$$

with probability $\frac{1}{2}$. Photon B is sent to Bob and photon A is left for Alice. There are two types of measurements that Alice may perform: she may measure along the rectilinear basis, thus distinguishing between horizontal and vertical photons. Alternatively, she may measure along the diagonal basis, thus distinguishing between the $+45^o$ and -45^o photons. Bob measures the polarizations at the other end. He measures in one of three bases, obtained by rotating rectilinear basis by angles $\phi_1 (\phi_1') = 0$, $\phi_2 (\phi_3') = \tan^{-1} \frac{\beta}{\alpha}$, $\phi_3 (\phi_2') = -\tan^{-1} \frac{\beta}{\alpha}$. The surperscript "$'$" refers to the case in which Alice chooses $|AB\rangle'$ as the original state.

The two users are connected by a quantum channel and a classical public channel. The quantum channel consists usually of an optical fiber. The public channel, however, can be any communication link. So how does this scheme work?

1. Alice and Bob pick a number $0 < \epsilon \leq 1$ and make its value public. The constraint on ϵ will be discussed in Sec. IV.

2. Alice sends a sequence of photons B from each pair in one of the two nonmaximally entangled states ($|AB\rangle$ and $|AB\rangle'$) chosen randomly and independently, and leaves the corresponding photons A. She also records her choice of $|AB\rangle$ or $|AB\rangle'$.

3. Alice has two types of measurements. One measurement along rectilinear basis (i.e., $\{|H\rangle, |V\rangle\}$) allows her to distinguish between horizontally and vertically polarized photons. The other measurement along diagonal basis (i.e., $\left\{\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\right\}$) allows her to distinguish between photons polarized at $+45^o$ and -45^o. Alice chooses between the two types with probabilities $1-\epsilon$ and ϵ, respectively. If she detects photon A in the state $|H\rangle$ or $\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, the result is 0; else, the measurement can yield the result 1, and potentially reveal one bit of information. She writes down her measurement bases and the results of the measurements.

4. For each photon, Bob performs measurements and registers the outcome of the measurements in one of three bases, obtained by rotating the rectilinear basis by angles $\phi_1 (\phi_1') = 0$, $\phi_2 (\phi_3') = \tan^{-1} \frac{\beta}{\alpha}$, $\phi_3 (\phi_2') = -\tan^{-1} \frac{\beta}{\alpha}$, i.e., $\{|H\rangle, |V\rangle\}$, $\{\alpha |H\rangle + \beta |V\rangle, \beta |H\rangle - \alpha |V\rangle\}$, and $\{\beta |H\rangle + \alpha |V\rangle, \alpha |H\rangle - \beta |V\rangle\}$, with probabilities $1-\epsilon$, $\frac{\epsilon}{2}$, and $\frac{\epsilon}{2}$, respectively. Similar to the measurements performed by Alice, each measurement can yield two results 0 (if he detects photon B in the state $|H\rangle$, $\alpha |H\rangle + \beta |V\rangle$ or $\beta |H\rangle + \alpha |V\rangle$) and 1 (if he detects photon B in the state $|V\rangle$, $\beta |H\rangle - \alpha |V\rangle$ or $\alpha |H\rangle - \beta |V\rangle$). The ensemble of these bits registered by both Alice and Bob is the raw key.

5. After exchanging enough photons, Bob announces on the public channel the sequence of bases he used, but not the results that he obtained.

6. Alice compares this sequence with the states that she originally chose, and the list of polarizations which she measured. Then she tells Bob on the public channel on which occasions his measurements have been done in the correct bases. Whenever Alice and Bob used the compatible basis, they should get perfectly correlated bits. However, due to imperfections in the setup, and to a potential eavesdropper, there will be some errors.

There are two cases in which Alice chooses entangled states $|AB\rangle$ and $|AB\rangle'$, respectively. For either of the two cases, both Alice and Bob are much more likely to choose the rectilinear basis and obtain correlated bits, thus achieving a significant gain in efficiency. If Alice chooses the diagonal basis, in order to generate a sifted key, Bob should choose between the bases $\{\alpha |H\rangle + \beta |V\rangle, \beta |H\rangle - \alpha |V\rangle\}$, and $\{\beta |H\rangle + \alpha |V\rangle, \alpha |H\rangle - \beta |V\rangle\}$ according to the entangled state chosen by Alice and the polarization of photon A. (Otherwise, if he uses the rectilinear basis, he gets

the outcomes 0 and 1 with probabilities $|\alpha|^2$ and $|\beta|^2$, respectively. These results abort.) Foe example, if Alice chooses the state $|AB\rangle$ and sends photon B to Bob. Then if she detects photon A polarized at $+45^o$ by measuring along the diagonal basis, Bob must choose the basis $\{\alpha|H\rangle+\beta|V\rangle, \beta|H\rangle-\alpha|V\rangle\}$ and photon B would be detected in the state $\alpha|H\rangle+\beta|V\rangle$. Therefore, they can generate a key bit "1" with probability $\frac{1}{2}\cdot\epsilon\cdot\frac{\epsilon}{2}$. The bases used by Alice and Bob agree with probability $(1-\epsilon)^2+\frac{\epsilon^2}{2}$ which goes to 1 as ϵ goes to *zero.*

Table I. Example of the case where Alice chooses $|AB\rangle$ as the original state. The measurement bases are presented as the angles by which the rectilinear basis is rotated (here $\theta=\tan^{-1}\frac{\beta}{\alpha}$). The two users choose a basis with certain probability to measure their particles and register the bit value (0 or 1), respectively. The ensemble of these bits is the raw key. Alice tells Bob on the public channel on which occasions his measurements have been done in the correct bases, and they keep only the bits corresponding to the compatible bases. This is the sifted key.

A basis	0	0	0	0	0	0	$\frac{\pi}{4}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$
A bit value	0	0	0	1	1	1	0	0	0	1	1	1
B basis	0	θ	$-\theta$	0	θ	$-\theta$	0	θ	$-\theta$	0	θ	$-\theta$
B bit value	0	1/0	1/0	1	1/0	1/0	1/0	0	1/0	1/0	1/0	1
compatible?	y	n	n	y	n	n	n	y	n	n	n	y
sifted key	0			1				0				1

7. For each of the two cases in which Alice chooses the entangled states $|AB\rangle$ or $|AB\rangle'$, Alice and Bob divide up their polarization data into twelve cases according to the actual bases used and the bit values yielded (shown in Table I), respectively. Then they throw away the eight cases when they have used non-compatible basis. Since the total probabilities for the two users to obtain the results 0 and 1 are equal, the ensemble of these bits of the remaining four cases is a sifted key. Hence, the remaining cases are kept for further analysis and to generate the secret key.

8. Alice and Bob divide up the accepted data into two subsets according to the entangled states originally chosen by Alice. From the subset where Alice chooses $|AB\rangle$ as the prior state, there are three cases. In one case where Alice and Bob both use the rectilinear basis (including two cases shown in Table I, in each of which the bit value is "0" or "1"), they randomly pick a fixed number say m_1 photons and publicly compare their polarizations. The number of mismatches r_1 (here, mismatch means the polarizations of photons are not correlated) tells them the estimated error rate $e_1=\frac{r_1}{m_1}$. In the case where Alice uses the diagonal basis and Bob uses the basis $\{\alpha|H\rangle+\beta|V\rangle, \beta|H\rangle-\alpha|V\rangle\}$, they pick a fixed number say m_2 photons and publicly compare their polarizations. The number of mismatches r_2 gives the estimated error rate $e_2=\frac{r_2}{m_2}$. In the case where Alice uses the diagonal basis and Bob uses the basis $\{\beta|H\rangle+\alpha|V\rangle, \alpha|H\rangle-\beta|V\rangle\}$, they pick a fixed number say m_3 photons and publicly compare their polarizations. The number of mismatches r_3 gives the estimated error rate $e_3=\frac{r3}{m_3}$. Similarly, from the subset where Alice chose $|AB\rangle'$ as the prior state, there are also three cases. Corresponding to the above discussion, we obtain the error rates $e_1'=\frac{r_1'}{m_1'}$, $e_2'=\frac{r_2'}{m_2'}$ and $e_3'=\frac{r_3'}{m_3'}$.

Note that the test samples m_1, m_1', m_2, m_2', m_3 and m_3' are sufficiently large, the estimated error rates e_1, e_1', e_2, e_2', e_3, and e_3' should be rather accurate [14,15]. Now they demand that e_1, e_1', e_2, e_2', e_3, and $e_3'<e_{\max}$ where $e_{\max}$ is a prescribed maximal tolerable error rate. If these independent constraints are satisfied, they proceed to the next steps. Otherwise, they throw away the polarization data and re-start the whole procedure. Notice that the constraints e_1, e_1', e_2, e_2', e_3, and $e_3'<e_{\max}$ are more stringent than the original naive prescription $\overline{e}<e_{\max}$ (here $\overline{e}$ is the average error rate). We will discuss it in detail in Sec. III.

9. Reconciliation and privacy amplification (see Ref. [1,13]).

III. REFINED ERROR ANALYSIS

For each photon, the eavesdropper, Eve does not know which nonmaximally entangled state it is chosen from. So for Eve, each photon is in an entangled mixed state. She has eavesdropping attack as below:

i). with a probability p_1 measures polarization of each photon along the rectilinear basis and re-sends a photon according to the result of her measurement to Bob;

ii). with a probability p_2 measures polarization of each photon along the basis $\{\alpha|H\rangle+\beta|V\rangle, \beta|H\rangle-\alpha|V\rangle\}$ and re-sends a photon according to the result of her measurement to Bob;

iii). with a probability p_3 measures polarization of each photon along the basis $\{\beta|H\rangle+\alpha|V\rangle, \alpha|H\rangle-\beta|V\rangle\}$ and re-sends a photon according to the result of her measurement to Bob;

iv). with a probability $1-p_1-p_2-p_3$ does nothing.

Eve has a whole set of eavesdropping strategies by varying the values of p_1, p_2 and p_3. Any of the strategies in this set is called "a biased eavesdropping attack" [13].

Consider the error rate e_1 (e_1') for the case both Alice and Bob use the rectilinear basis. For the biased eavesdropping strategy under current consideration, errors occur only if Eve uses the other two bases. This happens with a conditional probability p_2+p_3. In this case, the polarization of the photon is randomized, thus giving an error rate

$$e_1(e_1') = 2\alpha^2\beta^2\left(p_2+p_3\right). \tag{3}$$

Errors for the case where Alice uses the diagonal basis and Bob uses the basis $\{\alpha\left|H\right\rangle+\beta\left|V\right\rangle, \beta\left|H\right\rangle-\alpha\left|V\right\rangle\}$ occur only if Eve is measuring along the rectilinear basis or the basis $\{\beta\left|H\right\rangle+\alpha\left|V\right\rangle, \alpha\left|H\right\rangle-\beta\left|V\right\rangle\}$. This happens with a conditional probability p_1+p_3 and when it happens, the photon polarization is randomized. Thus, the error rate for this case is

$$e_2(e_3') = 2\alpha^2\beta^2 p_1 + 8\alpha^2\beta^2\left(\alpha^2-\beta^2\right)^2 p_3. \tag{4}$$

Similarly, errors for the case where Alice uses the diagonal basis and Bob uses the basis $\{\beta\left|H\right\rangle+\alpha\left|V\right\rangle, \alpha\left|H\right\rangle-\beta\left|V\right\rangle\}$ occur only if Eve is measuring along the rectilinear basis or the basis $\{\alpha\left|H\right\rangle+\beta\left|V\right\rangle, \beta\left|H\right\rangle-\alpha\left|V\right\rangle\}$. This happens with a conditional probability p_1+p_2. In this case, the error rate is given as

$$e_3(e_2') = 2\alpha^2\beta^2 p_1 + 8\alpha^2\beta^2\left(\alpha^2-\beta^2\right)^2 p_2. \tag{5}$$

Therefore, Alice and Bob will find that, for the biased eavesdropping attack, the average error rate

$$\begin{aligned}\overline{e} &= \frac{\left(1-\epsilon\right)^2\left(e_1+e_1'\right)+\frac{\epsilon^2}{4}\left(e_2+e_3+e_2'+e_3'\right)}{2\left[\left(1-\epsilon\right)^2+\frac{\epsilon^2}{2}\right]} \\ &= \frac{\alpha^2\beta^2\left[2\left(1-\epsilon\right)^2\left(p_2+p_3\right)+\epsilon^2 p_1+2\epsilon^2\left(\alpha^2-\beta^2\right)^2\left(p_2+p_3\right)\right]}{\left(1-\epsilon\right)^2+\frac{\epsilon^2}{2}}.\end{aligned} \tag{6}$$

Suppose Eve always eavesdrops only along rectilinear basis (i.e., $p_1=1$, $p_2=p_3=0$), then

$$\overline{e} = \frac{\alpha^2\beta^2\epsilon^2}{\left(1-\epsilon\right)^2+\frac{\epsilon^2}{2}} \to 0 \tag{7}$$

as ϵ tends to 0, which is similar with the result of Ref. [13]. This means that if Eve is always eavesdropping along the dominant basis, with a naive error analysis prescribed as $\overline{e} < e_{\max}$ Alice and Bob will fail to detect eavesdropping by Eve.

To ensure the security of our scheme, it is crucial to employ a refined data analysis: the accepted data are further divided into various subsets according to the actual basis used by Alice and Bob and the error rate of each subset is computed separately. In Sec. II, we have already computed the error rates e_1, e_1', e_2, e_2', e_3, and $e_3' < e_{\max}$ where $e_{\max}$ is a prescribed maximal tolerable error rate. From Eqs. (3,4,5), we can see that these error rates e_1, e_1', e_2, e_2', e_3, and e_3' depend on Eve's eavesdropping strategy and the degree of entanglement of the original state, but not on the value of ϵ. So the refined data analysis guarantees the security of the present scheme.

IV. THE CONSTRAINT ON ϵ

From the above discussion, we know the value of ϵ should be small but can not be *zero*. If ϵ were actually *zero*, the scheme would be insecure. The main constraint on ϵ is that there should be enough photons for an accurate estimation of the six error rates e_1, e_1', e_2, e_2', e_3, and e_3'. We assume that N entangled pairs are chosen by Alice, i.e., N photons are transmitted from Alice to Bob. On average, for $\left|AB\right\rangle$ or $\left|AB\right\rangle'$ only $N\epsilon^2/8$ photons belongs to each of the two cases where Alice uses the diagonal basis and Bob uses the basis $\{\alpha\left|H\right\rangle+\beta\left|V\right\rangle, \beta\left|H\right\rangle-\alpha\left|V\right\rangle\}$ or the basis $\{\beta\left|H\right\rangle+\alpha\left|V\right\rangle, \alpha\left|H\right\rangle-\beta\left|V\right\rangle\}$. To estimate e_2, e_2', e_3, and e_3' reasonably accurately, the number $N\epsilon^2/8$ should be larger than some fixed number say $m=\max\left(m_2, m_2', m_3, m_3'\right)$. The numbers m_2, m_2', m_3, and m_3' are the photon number needed for the refined error analysis, which can be computed from classical statistical analysis. So

$$\begin{aligned} N\epsilon^2/8 &\geq m, \\ \epsilon &\geq 2\sqrt{2m/N}. \end{aligned} \tag{8}$$

As N tends to ∞, ϵ can tend to *zero*, but never reach it. And the efficiency of this scheme is asymptotic 100%.

V. DISCUSSION AND CONCLUSION

From the refined error analysis, we find the error rates depend not only on Eve's eavesdropping strategy but also on the degree of entanglement of the original state. For the biased eavesdropping attack, the error rates e_i and e_i' ($i = 1, 2, 3$) are functions of $\alpha\beta$, the probability ϵ and the eavesdropping strategy of Eve (seeing Eqs. (3-5)). If Alice uses a product state as the original state, i.e., $\alpha\beta = 0$, whatever the probability ϵ and Eve's eavesdropping strategy are, the error rates e_i and e_i' equal to *zero*. That is, Alice and Bob will never detect eavesdropping by Eve whatever she does. In other words, if $\alpha\beta = 0$, the scheme is easily broken by an eavesdropper. The security of our scheme is relying on the degree of the entanglement of the original state. If $|\alpha\beta| = \frac{1}{2}$, this scheme is equivalent to an efficient "simplified EPR scheme" [3].

Of course, the QKD with nonmaximally entangled states may also be completed in another way. At first, the nonmaximally entangled state $|AB\rangle = \alpha|00\rangle + \beta|11\rangle$ (here $|\beta| < |\alpha|$) can be concentrated to an EPR state [16,17] with probability $2|\beta|^2$ [18]. If the concentration fails, EPR pairs are abandoned; else, they are used in an efficient "simplified EPR scheme" [3]. Obviously, the total efficiency of this QKD process should be no more than $2|\beta|^2$.

In summary, we propose a quantum key distribution (QKD) scheme based on entanglement, where Alice and Bob choose between various bases independently with substantially different probabilities. Since two parties are much more likely to be using the same basis, thus reducing the fraction of discarded data, a significant gain in efficiency is achieved. The efficiency can be tend to 100%, as the value of ϵ tends to *zero* (but can not reach it accurately).

To make the scheme secure against the dominant basis eavesdropping attack, it is crucial to have a refined error analysis in place of a naive error analysis. We separate the accepted data into various subsets according to the basis employed and estimate an error rate for each subset separately. It is only when all error rates are small enough that the security of transmission is accepted.

Acknowledgment

This work was supported by the National Natural Science Foundation of China.

[1] C. H. Bennett and G. Brassard, in *proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p.175.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1992).
[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[4] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[5] C. H. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin, J. Cryptol. **5**, 3 (1992).
[6] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000).
[7] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000).
[8] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[9] D. Dieks, Phys. Lett. **92**, 271 (1982).
[10] W. K. Wootters and W. Zurek, Nature (London) **299**, 802 (1982).
[11] J. S. Bell, Physics (Long Island City, N. Y.) **1**, 195 (1965).
[12] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[13] H.-K. Lo, H.-F. Chau, and M. Ardehali, arXiv: quant-ph/0011056.
[14] H.-K. Lo and H.-F. Chau, Science **283**, 2050 (1999).
[15] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[16] C. H. Bennett, H. J. Bernstein, S. Popescu and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[17] H.-K. Lo and S. Popescu, arXiv: quant-ph/9707038.
[18] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).